REMARKS

This paper is responsive to the Office Action dated January 25, 2006. All rejections of the Examiner are respectfully traversed. Reconsideration and further examination are respectfully requested.

At paragraphs 3 of the Office Action, the Examiner rejected claims 1-4, 6-8, 15-18, 20-22, 26-29, 31-37, 39-45 and 47-49 for anticipation under 35 U.S.C. 102, again citing United States patent number 5,748,736 of Mittra ("Mittra"). Applicants respectfully traverse this rejection.

Mittra discloses a system for secure multicast group communication via multicast or broadcast transmission. As shown in Figs. 1-3, a secure multicast group of Mittra covers a hierarchy of multicast networks. Mittra describes a secure multicast group consisting of senders, receivers, a group security controller (GSC), and at least one trusted intermediary (TI) server.

Beginning at line 61 of column 9, Mittra indicates the possible use of three types of keys to encrypt data. The first key type is a group key ("Kgrp") that is used to encrypt messages to the secure multicast group. Mittra states: "In this case, the sender encrypts the message with the group key and then multicasts the message." The Kgrp key is known to all members of the secure multicast group of Mittra. As noted by the Examiner, the secure multicast group of Mittra contains multiple multicast domains. The Kgrp key of Mittra is therefore known to members of multiple multicast domains.

A second key proposed for use by Mittra is one that is unique between a sender and the GSC ("Ksender-GSC"). This key agreed upon and known by only a single sender and the GSC. Mittra teaches that "[i]n this case, after encryption, the sender sends the message to the GSC

which decrypts the message and re-encrypts it with the current Kgrp before multicasting it." The Ksender-GSC key is "the key that the sender shares with the GSC for purposes of communicating over the secure channel, or any other key that the sender and the GSC agree on that is unique to that sender and the GSC." The Ksender-GSC key of Mittra is thus known only to the GSC and one sender. If Ksender-GSC is used for transmission from a sender to the GSC, then the GSC decrypts the message, and then re-encrypts the message using the Kgrp before retransmitting the message to the secure multicast group.

The third key disclosed in Mittra is Kencrypt, which is a "random key chosen by the sender . . . [that] must be changed after each message."

The above three encryption keys are described in columns 9 and 10 of Mittra.

Nowhere in Mittra is there disclosed or suggested any method or system of implementing multicast security in a given multicast domain, including:

> receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;
>
> decrypting the received multicast traffic with the global key to produce decrypted multicast traffic;
>
> ***encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to network devices in the given multicast domain, wherein the multicast domain includes a plurality of network devices, and wherein the multicast traffic includes a plurality of multicast messages***; and
>
> forwarding the local encrypted multicast traffic to the plurality of network devices in the given multicast domain. (emphasis added)

As in the present independent claim 1. Analogous features are also found in the present independent claims 15, 26, 34 and 42. As discussed above, the three keys of Mittra are either 1) known to all devices in a security group that includes multiple multicast domains (KGRP), 2) known only to an individual sender and the GSC (KSender-GSC), or 3) randomly generated on a

per message basis for use between an individual sender and the GSC. None of the keys described in Mittra disclose or suggest the ***local key*** of the present independent claims, that is used to encrypt ***decrypted multicast traffic to produce local encrypted multicast traffic, the local key being available only to network devices in the given multicast domain, wherein the multicast domain includes a plurality of network devices, and wherein the multicast traffic includes a plurality of multicast messages.***

In clear contradistinction, Mittra teaches away from any such key, stating with regard to Kgrp that "the current multicast group and the joining member all need to be apprised of the new Kgrp" (see column 8 of Mittra, lines 23-25). The Ksender-GSC key described by Mittra is "unique to that sender and the GSC" (see column 9 of Mittra, lines 15-17). Finally, the random key described beginning at line 36 of column 10 in Mittra "must be changed after each message." Accordingly, the three key options disclosed by Mittra are either 1) shared across multiple multicast domains (Kgrp), 2) unique to one sender and the GSC (KSender-GSC), or 3) uniquely generated by a sender on per message basis. Thus Mittra expressly teaches away from the local key of the present independent claims, that is used to encrypt ***decrypted multicast traffic to produce local encrypted multicast traffic, the local key being available only to network devices in the given multicast domain, wherein the multicast domain includes a plurality of network devices, and wherein the multicast traffic includes a plurality of multicast messages.***

For the reasons stated above, Applicants respectfully urge that Mittra does not disclose or suggest all the features of the present invention as set forth in independent claims 1, 15, 26, 34 and 42. Accordingly, Applicants respectfully submit that Mittra does not anticipate independent claims 1, 15, 26, 34 and 42 under 35 U.S.C. 102. As to claims 2-4, 6-8, 16-18, 20-22, 27-29, 31-

33, 35-37, 39-41, 43-45 and 47-49, they each depend from claims 1, 15, 26, 34 and 42, and are believed to be patentable over Mittra for at least the same reasons.

At paragraph 4, the Examiner rejected claims 9-14 and 23-25 as being obvious under 35 U.S.C. 103, citing the combination of United States patent number 6,331,983 of Haggerty et al. ("Haggerty et al.") and "The Microsoft Computer Dictionary", 5th Edition ("Microsoft Computer Dictionary"). Applicants respectfully traverse this rejection.

Haggerty et al. disclose a system for establishing connections in a switch-based communications network for multicast traffic. As described in Haggerty et al., a source receives a multicast packet on an access port from a source host, determines a group address in the multicast packet, and composes and sends a "sender present" message to other switches on its network ports. The receiving switches of the Haggerty et al. system then determine whether a local host wishes to join the group and if so, send a map message back toward the source switch on a predetermined path between the receiving switch and the source switch. The Microsoft Computer Dictionary discloses that encryption prevents unauthorized access, and that one or more keys may be used to perform encryption.

Like Mittra, the combination of Haggerty et al. and Microsoft Computer Dictionary also fails to disclose or suggest method or system of implementing multicast security in a given multicast domain, including:

> receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;
>
> decrypting the received multicast traffic with the global key to produce decrypted multicast traffic;
>
> ***encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to network devices in the given multicast domain, wherein the multicast domain includes a plurality of network***

devices, and wherein the multicast traffic includes a plurality of multicast messages; and

forwarding the local encrypted multicast traffic to the plurality of network devices in the given multicast domain. (emphasis added)

as in the present independent claims 1 and 15, from which claims 9-14 and 23-25 depend. Neither Haggerty et al. nor Microsoft Computer Dictionary include any hint or suggestion of even the desirability of having any local key that is shared by and specific to a multicast domain having a plurality of network devices, and that is used for a plurality of messages, as in the present independent claims.

For these reasons, Applicants respectfully urge that the combination of Haggerty et al. and Microsoft Computer Dictionary does not disclose or suggest all the features of the present independent claims 1 and 15, from which claims 9-14 and 23-25 depend. Accordingly, Haggerty et al. and Microsoft Computer Dictionary do not form a *prima facie* case of obviousness with regard to independent claims 1 and 15. As to claims 23-25 each depend from claims 1 and 15, they are respectfully believed to be patentable over Haggerty et al. and Microsoft Computer Dictionary for at least the same reasons. Reconsideration of all pending claims is respectfully requested.

For these reasons, and in view of the above amendments, Applicants respectfully request that the Examiner's rejections be withdrawn. This application is now considered to be in condition for allowance and such action is earnestly solicited.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone David A. Dagg, Applicants' Attorney at 617-630-1131 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

MARCH 21 2006
Date

David A. Dagg, Reg. No. 37,809
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-111